ABN: 37 145 128 436

Email Spoofing: Mitigating the Threat

What is Email Spoofing?

E-mail spoofing is the forgery of an e-mail so that the message appears to have originated from someone other than the actual source. Distributors of spam often use spoofing in an attempt to get recipients to open their solicitations.

Your email address can also be used to trick your customers and suppliers into responding. This is serious as it can damage the reputation of your business.

Mitigating the Threat

There is no single solution, but we do have some techniques available to increase the resilience of your email domain name when it comes to spoofing attacks.

Technique 1 – "SPF" Record

This is a DNS record published on the Internet for your company domain name.

The purpose of an SPF record is to prevent spammers from sending messages with forged "From" addresses at your domain.

More info: https://support.google.com/a/answer/33786?hl=en

Technique 2 – "DKIM" Record

This is another DNS record published on the Internet for your company domain name.

DomainKeys Identified Mail (DKIM) builds on SPF as another method designed to detect email spoofing. It uses cryptographic authentication to check that incoming mail is genuine.

More info: https://support.google.com/a/answer/174124?hl=en